(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2002 (10.01.2002)

PCT

(10) International Publication Number
WO 02/03291 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US01/20340

(22) International Filing Date: 27 June 2001 (27.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/609,043 30 June 2000 (30.06.2000) US

(71) Applicant: **REAL MEDIA, INC.** [US/US]; 580 Virginia Drive, Suite 200, Fort Washington, PA 19034 (US).

(72) Inventor: **BEYDA, Gil**; c/o Real Media, Inc., 580 Virginia Drive, Suite 200, Fort Washington, PA 19034 (US).

(74) Agent: **BLOOM, Allen**; Dechert, P.O. Box 5218, Princeton, NJ 08543 (US).

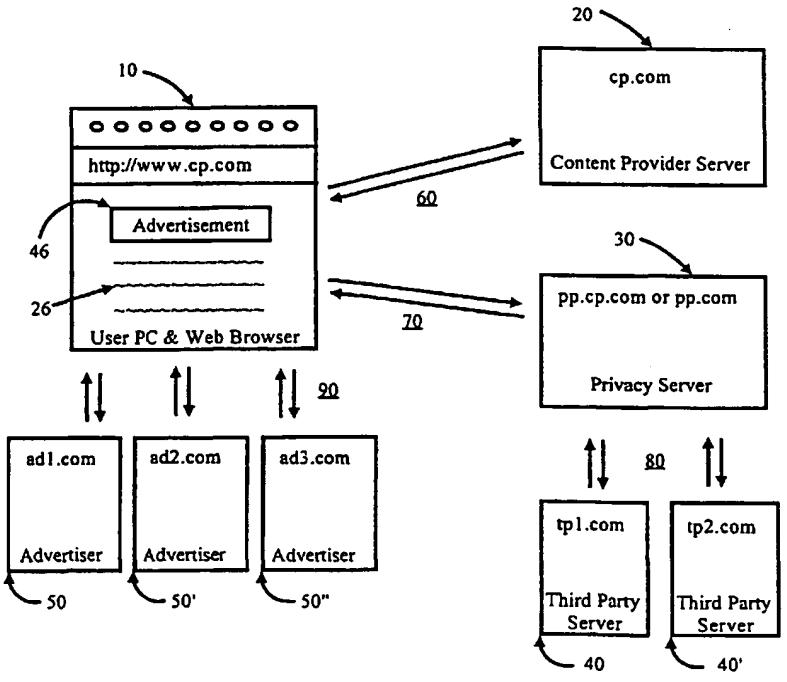
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR DELIVERING ADVERTISEMENT INFORMATION ON A DATA NETWORK WITH ENHANCED USER PRIVACY



(57) **Abstract:** The invention concerns a system and method for delivering advertisement information on a data network with enhanced user privacy. A user network processing device (10) is operable to transmit at least a first user request for resources (e.g., an HTTP request for an Internet World Wide Web page) and second user request for resources (e.g., based on an embedded HTML call to a third party for an advertisement) and present resources served in response to the first and second user requests for resources to the user. A first server (20) is operable receive the first user request for resources and transmit at least one first server resource to the user network processing device in response to the first user request for resources. A privacy server (30) is operable to receive the second user request for resources and transmit at least one privacy server resource (e.g., an advertisement) to the user network processing device in response to the second user request for resources; and a third party server (80) operable to receive a privacy server request for resources; and a third party server (80) operable to receive a privacy server request for resources and transmit at least one third party server resource (e.g., an advertisement) to the privacy server. The privacy server is operable to receive the third party server resource and generate the privacy server resource based on the third party server resource.

WO 02/03291 A1

SYSTEM AND METHOD FOR DELIVERING ADVERTISEMENT INFORMATION ON A DATA NETWORK WITH ENHANCED USER PRIVACY

The present invention relates to a system and method for delivering advertisement information via a data network while limiting the amount of information exchanged between a user (e.g., an Internet World Wide Web user) and an advertisement information provider.

In general, an Internet user accesses the World Wide Web (WWW or Web) using a network processing device such as personal computer and associated software including an operating system and Web Browser (e.g., Netscape Communicator, Microsoft Internet Explorer or the like). The Web Browser assists the user in identifying and/or inputting the network address of a given Web page or site. The address of a given Web site is generally formatted as a URL (Uniform Resource Locator), which is basically an advanced resource or file name formatted for Internet addressing. A URL typically points to a given resource such as an image or a file in a particular directory. The directory can exist on any machine on the Internet, and can be transmitted or served via one of many different protocols (e.g., HTTP, FTP, GOPHER, NEWS, NNTP, MAILTO and the like). However, typical World Wide Web documents are accessed using HTTP (Hyper-Text Transport Protocol).

A user can directly input the address of a given Web page into the address bar of the Web Browser (e.g., http://www.cp.com); where "cp" is the second level domain name and "com" is the top level domain of the requested Web site. In the alternative, the user can select a Web site from a pre-stored list of frequently visited sites (e.g., favorites or bookmarks). The user may also click on a Hyper-Text link embedded in a Web page (e.g., based on results returned from a typical search engine) or any other "Web-enabled" application (e.g., e-mail reader, news reader, word processor or the like) which contains a link to the desired site.

When an Internet user requests information from an Internet Web site, the Browser, via HTTP protocol, opens a connection and sends a request message to the desired Web server; the server then returns a response message, usually containing the resource (e.g., an HTML document) that was requested. After delivering the response, the server closes the connection. Often, the requested information arrives with an

embedded request to a third party server for advertisement information such as a banner ad. Some Web sites do not keep their advertisements locally. Rather, they subscribe to a third party advertisement service that places those ads for them. The third party typically serves advertisements for numerous advertisers and maintains a database that can correlate user information gathered from numerous advertising campaigns.

Advertisement information is transmitted to the user via an HTTP call to the third party server. When a typical Web page is requested, it is assembled through many HTTP requests by the user's Web Browser. First, there is a request for the HTML itself. Then, the user's Browser requests everything the Browser needs to build the page, including images, advertisement information, sounds, and plugins. The call to the third party server for advertisement information is typically an HTTP request for an image and is associated with a link to the advertiser's Web site. For example, the following HTML code fragment will present a typical "banner ad" (ad1.gif) to the user with its associated link to an advertiser (e.g., www.ad1.com). In this example, the image is served from a third party advertisement service located at tp1.com:

<A HREF="www.ad1.com">
<IMG SRC ="www.tp1.com/ad/ad1.gif">

In order to evaluate the performance of a given advertising campaign, it is desirable to collect advertisement statistics relating to the number of times the particular advertisement information is sent to a given user, the URL of the referring Web site, the number of times the user responds positively to the advertisement information (e.g., click throughs) as well as other information. However, in its basic form HTTP is a "stateless" (non-persistent) protocol, therefore it is difficult to differentiate between visits to a Web site and collect accurate advertisement statistics. In order to circumvent this problem, a Web server can tag or mark a user visiting its Web site. This is commonly achieved by storing "state" information called a cookie on the user's PC associated with the Web Browser. In its basic form a cookie contains an ID which is uniquely associated with the user and/or the user's Web Browser and is associated with a particular domain (i.e., the domain of the authoring Web site such as a third party advertisement service). Cookies typically contain various information stored in "name = value" paired format (e.g., ID = 123, Domain = cp.com, Age = 37 and the like).

Cookies can be written and read via variety of methods. However, in general, when a Web server sends a user a Web page it also sends header information that the

user's Browser records but does not display. Upon a first visit to a given Web site a Set-Cookie header is sometimes included with the Web page HTML. The Set-Cookie header specifies the "state" information that the Web site server wishes the user's Web Browser to record. When the user's Web Browser requests a page it also sends a variety of headers, specifying information such as the graphics formats it understands and the like. If a cookie has previously been set by a Web site that matches the desired URL the user's Web Browser adds a Cookie header quoting back the previously stored information.

Cookies can store database information, custom page settings, or just about anything that would make a site individual and customizable. For example, a cookie can contain an anonymous code given to the user so the Web site operator can see how many users return at a later time. These cookies are sometimes configured to stay on the user's system for months or years and are called "persistent" cookies. Some cookies contain a code specifically identifying the user (e.g., name, address, telephone number, age, e-mail address and the like). This usually occurs after the user registers with a particular Web site. The site then keeps a detailed account of pages visited, items purchased and the like, and can combine the information with information from other sources once the user has been identified. Some cookies contain a list of items the user has selected for purchase. This is often used in Web sites having a "shopping cart" to keep track of a user's order. Often cookies of this type 'expire' as soon as the user logs out or shortly thereafter. These are called "session" cookies. Some cookies contain personal preferences. These preference can be anonymous or can be correlated to personal information provided during user registration.

Once the HTTP request is made, the third party server typically returns an advertisement and a cookie (e.g., ID = 123, Domain = tp1.com). Or, if the third party server has previously written a cookie to the user, it receives the user's cookie with the HTTP request, reads the cookie and may use the information contained in the cookie along with other information to determine what advertisement to return in the response. The net result is that the user gets a cookie from the third party server without directly instructing the Browser to visit the third party Web site or domain.

The cookie provides an identifier that a third party can use to correlate a first request for information with subsequent requests. All of the information related to an advertising campaign and its associated cookie is typically maintained in a third party server database. Thus, a third party using this database gains a tool for correlating the

Internet user's information among all the parties to whom it provides advertising services or information.

For example, a user may access a Web site located at cp.com containing advertisements served by a third party server. The third party typically maintains a database that identifies the user by a unique ID, that the user accessed the cp.com Web site, and whether or not the user clicked through to the advertiser. If the user seeks content from cp2.com for which the third party also provides advertisement content, the third party will receive a previously written cookie (e.g., ID = 123 Domain = tp1.com) with its unique ID (123) correlated to the user. The third party can then correlate this information with all the prior information gathered from the user in connection with other advertising campaigns on cp.com or other Web sites.

Since many advertisements are served by a single third party advertisement service, user activity is easily correlated and tracked. When the user loads Web pages from various Web sites, every advertisement served by the third party server will result in an HTTP call to the third party server for the advertisement. Each HTTP call will return the cookie associated with the third party server's domain (identifying the user's ID). The third party server can also identify the referring Web site or domain by other means. Based on these and other pieces of information, the third party can compile a profile of a given user.

Various methods exist for tracking user information and preferences. For example, U.S. Patent No. 5,948,061 - Merriman et al. discloses a method of delivering targeted advertising including an advertising server process coupled as a node on a data network. The advertising server process stores advertisements for transmission upon user request and also gathers information from a user's Web Browser. Based on information passed by the user's Browser, the advertising server process determines the appropriate advertisement to transmit in response to the user's request. A database is maintained with information relating to a given advertising campaign including the number of times a user has seen a particular ad, the total number of times that ad has been shown as well as other information gathered after the user clicks on the ad.

Other systems and methods for serving or allocating advertisement information and gathering statistical information relating to Internet based advertisements are shown in U.S. Patent 5,796,952 - Davis et al., U.S. Patent No. 5,991,740 - Messer, U.S. Patent

6,006,197 - d'Eon et al. and U.S. Patent No. 6,026,369 - Capek. These references as well as U.S. Patent No. 5,948,061 are hereby incorporated by reference.

The amount of correlative information about the Internet user acquired by third parties quickly becomes substantial. Most of this data correlation is unknown to the Internet user. Spurred by growing concerns over unauthorized use of a user's information via the Internet, some users choose to proactively eliminate or at least severely limit the amount of information available to third parties. For example, a user may configure their Web Browser to refuse to accept cookies and/or the set the cookie file attributes "read-only". The user may also disable various Web Browser enhancements (e.g., ActiveX, Visual Basic Script, Java and JavaScript) further impeding a third party's ability to gather information from the user. These techniques often produce mixed results. Many Web sites do not operate properly without cookies. Further, some Web Browsers force the user to manually confirm that the user wishes to refuse a cookie each time the cookie is pushed by a third party server.

Other software based security programs are also available to assist the user in protecting personal information. While some or all of these security techniques may be effective, their usage is far from widespread. What is needed in the art, and provided by the invention, are simple and effective methods and devices, independent of the user, that allow third party providers, who are typically providers of advertisement information, data that meets their legitimate interest in monitoring the placement and success of their advertisements, while limiting their ability to gather and correlate an Internet user's data.

Summary of the Invention

The invention relates to a system and method for delivering advertisement information on a data network data with enhanced user privacy. A user network processing device is operable to transmit at least a first user request for resources (e.g., an HTTP request for an Internet World Wide Web page) and second user request for resources (e.g., based on an embedded HTML call to a third party for an advertisement) and present resources served in response to the first and second user requests for resources to the user. A first server is operable to receive the first user request for resources and transmit at least one first server resource to the user network processing device in response to the first user request for resources. A privacy server is operable to receive the second user request for resources and transmit at least one privacy server resource (e.g., advertisement data – an image or a pointer to an advertisement image) to the user network processing device in response to the second user request for resources; and a third party server operable to receive a privacy server request for resources and transmit at least one third party server resource (e.g., an advertisement) to the privacy server. The privacy server is operable to receive the third party server resource and generate the privacy server resource based on the third party server resource.

In a preferred embodiment the user network processing device has at least one memory area operable to store at least one user tag and the first server (optionally having a first server database) is operable to read data from the user tag, write data to the user tag (and optionally store data based on at least one of the user tag and the first user request for resources in the first server database). The user network processing device has at least one memory area operable to store at least one privacy server tag and the privacy server is operable to read data from the privacy server tag and write data to the privacy server tag. The third party server has a third party server database wherein the third party server is operable to read data from the privacy server tag, write data to the privacy server tag and store data based on at least one of the privacy server tag and the privacy server request for resources in the third party server database.

In an alternate embodiment, the privacy server has a privacy server database and at least one memory area operable to store at least one privacy server tag, the privacy server being operable to store in the privacy server tag data from the third party server and transmit the privacy server tag to the third party server.

In the context of the Internet, the user network processing device has a Web Browser having at least one associated memory area operable to store at least one user cookie and the first server has a first server database wherein the first server is operable to read data from the user cookie, write data to the user cookie and optionally store data based on at least one of the user cookie and the first user request for resources in the first server database.

In a preferred embodiment, the Web Browser has at least one memory area operable to store at least one privacy server cookie and the privacy server is operable to read data from the privacy server cookie and write data to the privacy server cookie. The third party server has a third party server database, the third party server being operable to read data from the privacy server cookie, write data to the privacy server cookie and store data based on at least one of the privacy server cookie and the privacy server request for resources in the third party server database.

In an alternate embodiment, the privacy server has a privacy server database and at least one memory area operable to store at least one privacy server cookie, the third party server being operable to read the data from the privacy server cookie and write data to the privacy server cookie.

Another aspect of the invention provides for a "Rich Media" third party server resource that is an image resource or an HTML resource having at least one embedded HTML call addressed to the third party server. The privacy server is operable to parse the HTML resource and rewrite the embedded HTML call to address the privacy server thereby providing support for Rich Media advertisements and the like.

In general, the privacy server is operable to (1) receive and identify a user request for resources directed to the privacy server as intended for forwarding to a third party server; (2) format a privacy server request for resources based on the user request for resources to the third party server; (3) transmit the privacy server request for resources; (4) receive a third party server resource from the third party server in response to the privacy server request for resources; and (5) transmit a privacy server resource based on the third party server resource.

The invention provides a simple and effective system and method, independent of the user, that allow third party providers, who are typically providers of advertisement information, data that meets their legitimate interest in monitoring the placement and

success of their advertisements, while limiting their direct access to an Internet user's personal data.

In general, communications between the user and other servers is carried out directly. However, the third party server does not communicate directly with the user. The privacy server relays data between the user and the third party server and eliminates a direct connection between the user and the third party server thereby limiting their ability to gather and correlate an Internet user's data.

Brief Description of the Drawings

Figure 1 is a general block diagram showing a user PC, content provider server, privacy server, third party servers and advertiser servers in data communication in accordance with the invention;

Figure 2 is a block diagram showing a user PC, content provider server, privacy server (located within the content provider Internet domain), third party server and an advertiser server in data communication in accordance with the invention;

Figure 3 is a flow chart showing the basic communication between a user PC, content provider server, privacy server and third party server accordance with the invention;

Figure 4 is a block diagram showing a user PC, content provider server, privacy server (located outside the content provider Internet domain), third party server and advertiser server in data communication in accordance with the invention; and

Figure 5 is a flow chart showing "Rich Media" enhanced communication between a user PC, content provider server, privacy server and third party server accordance with the invention.

Detailed Description of the Invention

Definitions

The following terms shall have, for the purposes of this application, the respective meanings set forth below.

- **Cookie:** as known in the art generally refers to a message or tag transmitted from a Web server and stored by a Web Browser. The Browser typically stores the cookie in a text file or directory. Each cookie typically contains one or more pieces of information in "name = value" paired format (e.g., ID = 123, Domain = cp.com, Age = 37 and the like). The cookie is then sent back to the Web server each time the Browser requests that page from the Web server.
- **Database:** as known in the art generally refers to a collection of information stored for later retrieval. Traditional databases are organized by fields, records, and files. A field is a single piece of information; a record is one complete set of fields; and a file is a collection of records. The term "database" is used herein in its broadest sense (i.e., a

collection of information) and is not limited to any particular structure or implementation.

• **Data network:** as known in the art generally refers to a group of two or more computer systems linked together in data communication. The term "data network" encompasses any type of wired or wireless computer network, independent of protocol, including local-area networks (LANs), wide-area networks (WANs) and networks of networks including the an intranet, extranet and the Internet.

• **HTML:** as known in the art is an acronym for Hyper-Text Markup Language, the authoring language used to create documents on the World Wide Web. HTML defines the structure and layout of a Web document by using a variety of tags and attributes.

• **Rich Media:** as known in the art refers to Internet advertisements or banners containing anything including an image file. Rich Media types include Shockwave, Flash or Java banners, as well as various other lesser-known types of media; and HTML elements including but not limited to frames, iframes, layers and ilayers which allow inclusion of external objects including other HTML documents into a Web page.

• **Img:** as known in the art generally refers to an HTML element that defines how an inline image is displayed by a Web Browser. The Img element generally defines the size and location of the image within a Web page and typically supports various image formats such as PNG, GIF and JPEG.

• **Link:** as known in the art generally refers to an HTML element that provides a Hyper-Text link. For example an HTML element supporting the HREF attribute which specifies a Hyper-Text link to another resource, such as an HTML document, image or the like.

• **Network processing device:** as known in the art generally refers to a network processing location or node. A network processing device includes but is not limited to a computer (such as a PC) portable or hand held computer device, other network enabled device (such as a Browser phone), or some other device, such as a printer. Each network processing device is typically assigned a unique static or dynamically assigned network address.

• **Resource:** as known in the art generally refers to any hardware or software item that can be used on a network. The term as it is recited herein primarily refers to data,

pointers to data, routines or pointers to routines that are available to network processing devices such as network servers, peers and/or clients (i.e., Web Browsers) and the like.

• **Server:** as known in the art generally refers to a program running on a computer which provides some service to other (e.g., client) programs.

It is understood that all references to Internet domain names such as cp.com, tp1.com, pp.com, ad1.com and the like are used herein for illustrative purposes only. These domain names have no correlation to any individual or business entity with an identical or similar Internet domain name previously or currently in use on the Internet or any individual or business entity adopting an identical or similar Internet domain name in the future.

The invention concerns a data network communication system and method for presenting resources to a user. The terms "present" or "presenting" as used herein are used in their ordinary sense and include displaying or playing audio and/or visual information to a user. The data network generally includes a plurality of nodes such as a user network processing device, content provider server, privacy server, third party server, and an advertiser server coupled in data communication. The term "coupled" as recited herein is used in its broadest sense and does not require a physical connection between devices. Two or more devices as disclosed herein are "coupled" so long as data communication between the devices is possible (e.g., hard wired data communication, wireless data communications and the like).

In the context of the Internet, many types of network servers are available to provide resources to a user such as those for Network File System, Network Information Service (NIS), Domain Name System (DNS), FTP, news, finger, Network Time Protocol. The connection between two network nodes or a client and server is normally by means of message passing, over the data network, and uses some protocol (such as TCP/IP) to encode the client's requests and the server's responses. Typical servers may run continuously (as a daemon), waiting for requests to arrive or may be invoked by some higher level daemon which controls a number of specific servers.

The term "user network processing device" generally refers to any user operable device having access to the data network including but not limited to a personal computer (portable or desktop), personal digital assistant (PDA), Browser phone, 2-way pager or the like. The user network processing device can be operated by an individual or may be programmed to operate automatically (i.e., timed schedule or triggered by an

external event). Thus, the term "user" as recited herein encompasses an individual as well as a computerized device operable to access the data network and perform computer automated functions.

In the context of the Internet, the user network processing device, content provider server, privacy server, third party server and advertiser server all communicate via TCP/IP protocol (Transmission Control Protocol over Internet Protocol). Each is network addressable in that it has a specific IP address (i.e., the 32-bit address defined by the Internet Protocol usually represented in dotted decimal notation) which is used to route data between the devices. The third party server and privacy server are preferably coupled to the Internet via high speed access methods (e.g., T1 (1.544 Mbps), T3 (44.736 Mbps), OC-3c (155Mbps), OC-12c (622Mbps) and the like). High speed communication between the third party server and privacy server is desirable so that maximum network performance is maintained.

The user network processing device is operable to transmit a plurality of user requests for resources and present the resources served in response to the user. The content provider server (first server) is operable to receive a first user request for resources and transmit a content provider server resource to the user network processing device in response. The privacy server is operable to receive a second user request for resources and transmit a privacy server resource to the user network processing device in response. The privacy server is also operable to transmit a privacy server request for resources based on the second user request for resources. The third party server is operable to receive the privacy server request for resources and transmit a third party server resource to the privacy server. The privacy server is operable to receive the third party server resource and generate the privacy server resource based on the third party server resource (e.g., a pointer to an image). In general, communications between the user and other servers is carried out directly. However, the third party server does not communicate directly with the user. The privacy server relays data between the user and the third party server and eliminates a direct connection between the user and the third party server thereby limiting the amount of data that is transmitted to the third party and ultimately correlated with the user.

Figure 1 shows a general block diagram of a user network processing device (user PC and Web Browser 10), content provider server (first server) 20, privacy server 30, third party servers 40 and 40' and advertiser servers 50, 50' and 50'' in data

communication via the Internet in accordance with the invention. Figure 1 generally shows the data communications paths between the user PC and Web Browser 10, content provider server 20, privacy server 30 and third party servers 40, 40' and advertiser servers 50, 50', 50'' in loading a typical Web page containing an advertisement 46 served by third party server 40 and content 26 server by content provider server 20.

Communications between user PC and Web Browser 10, content provider server 20, privacy server 30 and advertisement servers 50, 50'and 50'' are generally shown by arrows 60, 70 and 90. Communication between the privacy server 30 and third party servers 40 and 40' are generally shown by arrows 80 It is understood that data communications via the Internet often traverse a series of intermediate network nodes prior to reaching the desired destination (e.g., the user or the first provider Web site). Arrows 60, 70, 80 and 90 do not suggest a direct physical connection between the user PC and Web Browser 10 and/or various servers and encompass typical Internet communications (a connectionless, best-efforts packet-based system). It is also understood that other data networks using various network protocols are suitable for use in accordance with the invention.

The user PC and Web Browser 10 is operable to accesses the Internet World Wide Web (WWW or Web). The user PC preferably has an associated operating system such as Microsoft Windows or Linux and includes a typical Web Browser such as Netscape Communicator (for Windows or Linux) or Microsoft Internet Explorer, as well as numerous others. The Web Browser assists the user in requesting and displaying Web pages or sites containing desired information. The hardware and software configuration of a user network processing device for Internet access is routine and generally known to those skilled in the art.

The first provider server 20 and advertiser servers 50, 50', 50'' are preferably HTML servers hosting a Web site (e.g., cp.com, ad1.com). There are many varieties of commercially or publicly available World Wide Web server software packages which are compatible with the invention (e.g., Apache, IBM WebSphere products, NETSCAPE Enterprise, Microsoft Windows IIS Server and the like) all of which can be implemented with commonly available hardware from vendors such as IBM, Hewlett Packard, Compaq, Dell, Sun and numerous others that are known to those skilled in the art.

Similarly, privacy server 30 is preferably an HTML server and can be at least partially implemented using commercially or publicly available World Wide Web server

software and commonly available hardware from vendors such as IBM, Hewlett Packard, Compaq, Dell, Sun and numerous others that are known to those skilled in the art. The specific function of the privacy server is set forth in more detail below.

Third party servers 40 and 40' are also preferably HTML servers operable to serve or transmit advertisement information in response to requests for resources. Typical third party servers transmit advertisement information to a user for presentation as part of a Web page. Third party servers are usually maintained by an advertisement service or the like which assists one or more advertisers in publicizing various goods and/or services. Each advertiser will typically have its own Web site that can be accessed by the user in response to the advertisement information displayed by the user's Web Browser (e.g., via an HTML link to the advertiser's Web site).

Figure 2 is a more detailed block diagram showing a user PC and Web Browser 10, content provider server 20, privacy server 30 (located within the content provider domain), third party server 40 (third server) and an advertiser server 50 in data communication in accordance with the invention. Figure 2 generally shows the data communications paths between the user PC and Web Browser 10, content provider server 20, privacy server 30, third party server 40 and advertiser server 50 in loading a typical Web page containing content from the content provider server 20 and an advertisement 46 served by third party server 40. Advertiser server 50 may optionally include a database 52 operable to record information relating to one or more advertisement campaigns. It is generally understood that when the user clicks on the advertisement 46, the user's Web Browser is directed to the advertiser's web site. This may also involve the user's Web Browser being directed to several intermediate servers for click through tracking.

Figure 2 shows an excerpt of the user's cookie memory 12 (typically RAM and/or a file or directory). The first cookie (TP-ID = 123, Domain = tp1.com) represents a cookie which the user received from the third party server 40 without the benefit of a privacy server 30. The third party server 40 authored or wrote the cookie to the user's Web Browser and will receive the cookie back each time the user requests resources directly from the third party server. The third party server is also able to identify the referring domain and track the user's movement from all Web sites having ads served by the third party server 40.

The second cookie (CP-ID = 234, Domain = cp.com) represents a cookie authored by the content provider server 20. The content provider server will receive this cookie each time the user requests resources from the content provider server. The third cookie (PP_tp1.com_TP-ID = 345, Domain = cp.com) represents a cookie authored by the privacy server 30 and is discussed in more detail below. As shown in Figure 1, the privacy server is located within the content provider server domain (cp.com).

Operation of a system and method in accordance with the invention is best understood with reference to Figures 2 and 3. In general, the foregoing example outlines communications involved in a user accessing a Web site served from a content provider located at cp.com. The user's Web Browser checks the user's cookie memory 12 and locates the cookie associated with the cp.com domain. If the user has never visited the cp.com Web site, no cookie will exist. In this example, the content provider server 20 previously assigned the user an ID (e.g., CP-ID = 234) and returned this information in a cookie with a previously requested content provider resource. The user ID along with other information related to the user is recorded in an optional content provider server database 22. See Figure 2, content provider database excerpt 24 (e.g., also showing the third party server domain – tp1.com and advertiser domain ad1.com). The cookie is stored in the user's cookie memory 12 and is associated with the cp.com domain.

The user's Web Browser sends a first user request for resources (e.g., an HTML document) to cp.com. See Figure 3, block 100. The first user request for resources will be accompanied by any cookie information associated with the user and the cp.com domain in subsequent requests to the content provider server 20 (e.g., in an HTTP header). The content provider server receives the user request for resources (and cookie if present) and returns a content provider resource (e.g., the HTML document for the cp.com Web site). See Figure 3, block 110.

The user's Web Browser receives the content provider resource (i.e., the HTML document) and begins building the Web page for presentation (e.g., audio and/or visual) to the user. In this case, the requested resource includes an embedded request for resources, namely advertisement information ultimately served by the third party server 40. However, instead of requesting the advertisement information from the third party server 40, the first provider server pre-formats the embedded request for resources for the privacy server 30. This can be accomplished by several methods such as rewriting the content provider's HTML code to direct all requests for resources intended for the third

party server to the privacy server 30 as shown in the following exemplary HTML code fragments:

1) Original HTML code for third party server ad with click trough tracking:

```
<A HREF="www.tp1.com/ad/ad1">
<IMG SRC ="www.tp1.com/ad/ad1.gif"></A>
```

2) HTML code rewritten for content provider click through tracking:

```
<A HREF="www.cp.com/.../www.tp1.com/ad/ad1">
<IMG SRC ="www.tp1.com/ad/ad1.gif"></A>
```

3) HTML code rewritten by content provider for privacy server:

```
<A HREF="pp.cp.com/www.cp.com/.../www.tp1.com/ad/ad1">
<IMG SRC ="pp.cp.com/www.tp1.com/ad/ad1.gif"></A>
```

The original HTML code as set out above in example 1 includes an "A Href" call which is a link to an advertiser (ad1.com) via the third party server, tp1.com, so that click throughs can be tracked by the third party server. An "Img Src" call also identifies the location of a banner ad on the third party server. The content provider typically rewrites the original HTML code to include click through tracking via the content provider server. As shown above in example 2, this can be accomplished by rewriting the "A Href" call to a click through address associated with the content provider server. This type of HTML rewriting is known to those skilled in the art.

Support for the privacy server, in accordance with the invention, is provided by rewriting the "Img Src" call to point to the privacy server 30 (e.g., pp.cp.com). As shown in Figure 2, the privacy server is located within the content provider server domain (cp.com). In the alternative, the privacy server can be located within a separate domain (e.g., pp.com) as discussed in more detail below with reference to Figure 4. The "A Href "call may also be rewritten to include click through tracking via the privacy server. As shown above in example 3, this can be accomplished by rewriting the "A Href "call to a click through address associated with the privacy server. The rewriting of the content provider's HTML code is independent of the user and requires no user intervention. Rewriting can be done at the time the content provider resource is authored

or can be re-written on the fly via a process running on the content provider server prior to transmitting the content provider resource.

In processing the content provider resource, the user's Web Browser again checks the user's cookie memory 12 and locates any cookies associated with the privacy server domain. Since the privacy server is located within the content provider domain, the user's Web Browser will send any cookie associated with the cp.com domain to the content provider server 20 as well as the privacy server 30. Some of the cookie "name = value" pairs will be authored by the content provider server 20, others will be authored by the privacy server 30. Preferably, the content provider server 20 and privacy server 30 author distinct "name = value" pairs so that no cookie data is corrupted. In operation, the content provider server 20 will receive and ignore "name = value" pairs authored by the privacy server 30. Similarly, the privacy server 30 will receive and ignore "name = value" pairs authored by the content provider server 20.

The privacy server 30 can optionally include a privacy server database 32 as shown in more detail by privacy server database excerpts 34. If the privacy server 30 includes a database, various data mapping and logging operations are possible. For example, the privacy server database can correlate the privacy server user ID with the Third party server user ID (e.g., PP-ID = 345, TP-ID = 456, Domain = tp1.com). The privacy server can also include a performance log to monitor the response time of the third party server 40 in association with a particular advertising campaign (e.g., Third Party = tp1, Advertisement = ad1, performance or response time = 1 second). The function of the performance log is discussed in more detail below.

The user's Web Browser transmits a second user request for resources to the privacy server (seeking the image associated with the embedded "Img Src" call). See Figure 3, block 120. Communications between the user PC and Web Browser 10 and the privacy server 30 are shown generally by arrows 70. The privacy server 30 receives the second user request for resources (and cookie if present). In this example, the privacy server receives the HTTP request for an image that ultimately resides on the third party server 40 (e.g., pp.cp.com/www.tp1.com/ad/ad1.gif). The privacy server formats a request for resources (for the third party server) based on the second user request for resources by stripping the privacy server (pp.cp.com) portion of the HTTP request and requesting the image (ad1.gif) from the third party server 40 at the designated URL (www.tp1.com/ad/ad1.gif).

The first time the privacy server 30 requests resources from the third party server 40, the third party will assign the user (via the privacy server) a new user ID and send a cookie (e.g., TP-ID=345, Domain = tp1.com). The user ID along with other information related to the user is recorded in the third party database 42. Rather than store the cookie, the privacy server is operable to rewrite the cookie and store it on the user PC & Web Browser 10. See Figure 3, block 130. The privacy server embeds the third party cookie information (associated with the tp1.com domain) into a privacy server cookie having a new "name = value" pair associated with the privacy server domain, cp.com (e.g., PP_tp1.com_TP-ID = 345, Domain = cp.com).

In subsequent requests for resources to the third party, the privacy server receives the privacy server cookie, re-formats the information (e.g., TP-ID = 345, Domain = tp1.com). The URL of the third party resource (www.tp1.com/ad/ad1.gif) is based on or derived from the content provider server resource (HTML). The privacy server strips the URL from the "Img Src" call and transmits a privacy server request for resources to the third party server 40 and includes the re-formatted privacy server cookie. See Figure 3, block 140. Communications between the privacy server 30 and the third party server 40 are shown generally by arrows 80.

The third party server 40 receives the privacy server request for resources and cookie and returns a third party resource (e.g., advertisement data – an image or a pointer to a banner ad for advertiser ad1). See Figure 3, block 150. The privacy server 30 receives the third party server resource and generates the privacy server resource based on the third party server resource. In a preferred embodiment, the privacy server returns a copy of the third party server resource (e.g., an image or a pointer to an image). See Figure 3, block 160. The user receives the privacy server resource and presents it to the user as part of the cp.com Web page. See Figure 3, block 170.

As discussed above, Figure 2 shows a user cookie having and TP-ID = 123 associated with tp1.com. This cookie was authored by the third party server 40 and is typically used by the third party to track all of the user's activities relating to all third party served advertising campaigns. However, all advertising information provided via the privacy server is not correlated to the user since the third party server 40 associates at least a portion of the user's activity to a different user (TP-ID = 345). The third party cannot correlate TP-ID = 123 with TP-ID = 345. No user intervention is required to disassociate the user's "privacy server ID" from the user's actual third party ID.

Figure 2 also shows other information contained within the various server databases. The third party server typically tracks whether a given user clicks through to the advertiser's Web site. This can be accomplished by conventional methods not shown. The occurrence of click throughs (CT) is generally shown in the third party database excerpt 44. The third party database excerpt shows that the user was also presented with advertisements for advertiser ad2. Another user, TP-ID 567 (CP-ID = 456) also visited the cp.com Web site and was shown an advertisement for advertiser ad1 (via the privacy server). See the content provider database excerpt 24, privacy server database excerpt 34 and the third party database excerpt 44.

As discussed above, the privacy server can also monitor the performance of the third party server. In a preferred embodiment, the privacy server is operable to measure a time interval between the transmission of the privacy server request for resources and receipt of the third party server resource. This "performance measurement" can be stored in the performance log (e.g., part of the privacy server database).

The privacy server 30 can optionally transmit a second privacy server request for resources to another third party server (fourth server) if the time interval is greater than a performance criterion. See e.g., tp2.com - Figure 1. For example, the privacy server may seek an alternate source of resources if the third party server does not respond with 5 seconds. In this case, the privacy server resource is "based on" non-receipt of the third party resource as well as another third party resource. In the alternative, the privacy server 30 can transmit a second privacy server request for resources to the content provider server if the time interval is greater than a performance criterion. In this case, the privacy server resource is "based on" non-receipt of the third party resource as well as a substitute resource served by the content provider.

The privacy server 30 can optionally initiate a corrective action if the time interval is greater that a performance criterion. For example, the privacy server can send a notification to the third party server (e.g., an e-mail message). The privacy server can also notify a privacy server administrator (e.g., a notification displayed on a computer monitor, an e-mail or the like).

Figure 4 shows an alternative embodiment in which the privacy server is located outside of the first provider server domain. In general, communications between the various servers and the user PC and Web Browser Operation are carried out as discussed with reference to Figure 3. Figure 4 shows an excerpt of the user's cookie memory 12.

The first cookie (TP-ID = 123, Domain = tp1.com) represents a cookie which the user received from the third party server 40 without the benefit of a privacy server 30'. The third party server 40 authored or wrote the cookie to the user's Web Browser and will receive the cookie back each time the user requests resources directly from the third party server. The third party server is also able to identify the referring domain and track the user's movement from all Web site's having ads served by the third party server 40.

The second cookie (CP-ID = 234, Domain = cp.com) represents a cookie authored by the content provider server 20. The content provider server will receive this cookie each time the user requests resources from the content provider server. The third cookie (PP-ID = 345, Domain = pp.com) represents a cookie authored by the privacy server 30. As shown in Figure 4, the privacy server 30' is located within a separate domain (pp.com).

Referring to Figures 3 and 4, the user's Web Browser checks the user's cookie memory 12 and locates the cookie associated with the cp.com domain. If the user has never visited the cp.com Web site, no cookie will exist. In this case the content provider server 20 assigns the user an ID (e.g., CP-ID = 234) and returns a cookie with the content provider resource. The user ID along with other information related to the user is recorded in the content provider server database 22. See Figure 4, content provider database excerpt 24 (e.g., also showing the third party server domain – tp1 and advertiser domain ad1). The cookie is stored in the user's cookie memory 12 and is associated with the cp.com domain.

The user's Web Browser sends a first user request for resources (e.g., an HTML document) from cp.com. See Figure 3, block 100. The first user request for resources will be accompanied by any cookie information associated with the user and the cp.com domain in subsequent requests to the content provider server 20 (e.g., in an HTTP header). The content provider server receives the user request for resources and cookie and returns a content provider resource (e.g., the HTML document for the cp.com Web site). See Figure 3, block 110.

The user's Web Browser receives the content provider resource (i.e., the HTML document) and begins building the Web page for presentation (e.g., audio and/or visual) to the user. In this case, the requested resource includes an embedded request for resources, namely advertisement information ultimately served by the third party server 40. However, instead of requesting the advertisement information from the third party

server 40, the first provider server pre-formats the embedded request for resources for the privacy server 30'. This can be accomplished by rewriting the content provider's HTML code to direct all requests for resources intended for the third party server to the privacy server as shown in the following exemplary HTML code fragments:

1) Original HTML code for third party server ad with click trough tracking:
<A HREF="www.tp1.com/ad/ad1">
<IMG SRC ="www.tp1.com/ad/ad1.gif"></A>

2) HTML code rewritten for content provider click through tracking:
<A HREF="www.cp.com/.../www.tp1.com/ad/ad1">
<IMG SRC ="www.tp1.com/ad/ad1.gif"></A>

3) HTML code rewritten by content provider for privacy server:
<A HREF="pp.com/www.cp.com/.../www.tp1.com/ad/ad1">
<IMG SRC ="pp.com/www.tp1.com/ad/ad1.gif"></A>

The original HTML code as set out above in example 1 includes an "A Href" call which is a link to an advertiser (ad1) via the third party server, tp1.com, so that click throughs can be tracked by the third party server. An "Img Src" call also identifies the location of a banner ad on the third party server. The content provider typically rewrites the original HTML code to include click through tracking via the content provider server. As shown above in example 2, this can be accomplished by rewriting the "A Href" call to a click through address associated with the content provider server.

Support for the privacy server, in accordance with the invention, is provided by rewriting the "Img Src" call to point to the privacy server 30'. As shown in Figure 4, the privacy server is located within a separate domain (pp.com). The "A Href" call may also be rewritten to include click through tracking via the privacy server. As shown above in example 3, this can be accomplished by rewriting the "A Href" call to a click through address associated with the privacy server. The rewriting of the content provider's HTML code is independent of the user and requires no user intervention. Rewriting can be done at the time the content provider resource is authored or can be re-written on the

fly via a process running on the content provider server prior to transmitting the content provider resource.

In processing the content provider resource, the user's Web Browser again checks the user's memory 12 and locates any cookies associated with the privacy server domain. Since the privacy server is located outside of the content provider domain, the user's Web Browser will not send any cookie associated with the cp.com domain to the privacy server 30'.

As shown in Figure 4, the privacy server 30' can include a privacy server database 32' as shown in more detail by privacy server database excerpts 34'. Using database 32' various data mapping and logging operations are possible. For example, the privacy server database 32' can correlate the privacy server user ID with the Third party server user ID (e.g., PP-ID = 345, TP-ID = 456, Domain = tp1.com). The privacy server can also include a performance log to monitor the response time of the third party server 40 in association with a particular advertising campaign (e.g., Third Party = tp1, Advertisement = ad1, performance or response time = 1 second). The function of the performance log is discussed in more detail with reference to Figure 2 above.

The user's Web Browser transmits a second user request for resources to the privacy server (seeking an image associated with the embedded "Img Src" call). See Figure 3, block 120. Communications between the user PC and Web Browser 10 and the privacy server 30' are shown generally by arrows 70. The privacy server 30' receives the second user request for resources (and cookie if present). In this example, the privacy server receives the HTTP request for an image that ultimately resides on the third party server 40 (e.g., pp.com/www.tp1.com/ad/ad1.gif). The privacy server formats a request for resources (for the third party server) based on the second user request for resources by stripping the privacy server (pp.cp.com) portion of the HTTP request and requesting the image (ad1.gif) from the third party server 40 at the designated URL (www.tp1.com/ad/ad1.gif).

The first time the privacy server 30' requests resources from the third party server 40, the third party will assign the user (via the privacy server) a new user ID and send a cookie (e.g., TP-ID=345, Domain = tp1.com). The user ID along with other information related to the user is recorded in the third party database 42. The privacy server 30' is operable to maintain any cookies written by the third party server (normally intended for the user). These "privacy server" cookies can be stored by the privacy server in the same

fashion as the cookies stored by the user's Web Browser. For matters of simplicity, the information stored in "privacy server" cookies is shown as part of the privacy server database.

In subsequent requests for resources to the third party, the privacy server retrieves the privacy server cookie from the privacy server database 32'. The privacy server transmits a privacy server request for resources to the third party server 40 and includes the privacy server cookie. See Figure 3, block 140. Communications between the privacy server 30 and the third party server 40 are shown generally by arrows 80.

The third party server 40 receives the privacy server request for resources (and cookie if present) and returns a third party resource (e.g., advertisement data – an image or a pointer to a banner ad for advertiser ad1). See Figure 3, block 150. The privacy server 30 receives the third party server resource and generates the privacy server resource based on the third party server resource. In a preferred embodiment, the privacy server returns a copy of the third party server resource (e.g., an image or a pointer to an image). See Figure 3, block 160. The user receives the privacy server resource and presents it to the user as part of the cp.com Web page. See Figure 3, block 170.

As discussed above, Figure 4 shows a user cookie having and TP-ID = 123 associated with tp1.com. This cookie was authored by the third party server 40 and is typically used by the third party to track all of the user's activities relating to all third party served advertising campaigns. However, all advertising information provided via the privacy server is not correlated to the user since the third party server 40 associates at least a portion of the user's activity to the user TP-ID = 345. The third party cannot correlate TP-ID = 123 with TP-ID = 345 and no user intervention was required.

Figure 4 also shows other information contained within the various server databases. The third party server typically tracks whether a given user clicks through to the advertiser's Web site. This can be accomplished by conventional methods not shown. The occurrence of click throughs (CT) is generally shown in the third party database excerpt 44. The third party database excerpt shows that the user was also presented with advertisements for an advertiser located at ad2.com. Another user, TP-ID 789 (CP-ID = 678) also visited the cp.com Web site and was shown an advertisement for ad1.com (via the privacy server). See the content provider database excerpt 24, privacy server database excerpt 34' and the third party database excerpt 44.

The privacy server 30' can optionally transmit a second privacy server request for resources to a second third party server (e.g., see tp2.com - Figure 1) if the time interval is greater than a performance criterion. For example, the privacy server may seek an alternate source of resources if the third party server does not respond with 5 seconds. In this case, the privacy server resource is "based on" a second third party resource as well as the fact that the third party server resource was not received..

In another embodiment of the invention, the third party resource is displayed to the user using Rich Media such as an Iframe, which defines an inline frame for the inclusion of external objects including other HTML documents and/or images. Rich Media is advantageous in that it can present to the user an enhanced advertisement having animation and other eye catching effects.

Referring to Figures 2 and 5, a typical Rich Media advertisement is initiated by an HTML call to a third party server. See Figure 5, block 200. The content provider returns an HTML document including an embedded request for resources to a third party server. See Figure 5, block 210. As discussed above, the content provider server will rewrite the HTML call to request third party resource via the privacy server 30 as shown below:

1) Original HTML code for Rich Media ad:

<IFRAME SRC="www.tp1.com/ad/ad1.html" Height=60 Width=468>

2) HTML code rewritten by content provider:

<IFRAME SRC="pp.cp.com/www.tp1.com/ad/ad1.html" Height=60 Width=468>

Unlike a simple banner ad, the HTML call is a request for an HTML document (rather than an image). In processing the content provider resource, the user's Web Browser checks the user's memory 12 and locates any cookies associated with the privacy server domain. Assuming the privacy server is located within the content provider domain, the user's Web Browser will send any cookie associated with the cp.com domain to the content provider server 20 as well as the privacy server 30.

The user's Web Browser transmits a second user request for resources to the privacy server (seeking an HTML document associated with the embedded "Iframe Src"

call). See Figure 5, block 220. The privacy server 30 receives the second user request for resources (and cookie if present). In this example, the privacy server receives the HTTP request for an HTML document that ultimately resides on the third party server 40 (e.g., pp.cp.com/www.tp1.com/ad/ad1.html). See Figure 5, block 230. The privacy server formats a request for resources (for the third party server) based on the second user request for resources by stripping the privacy server (pp.cp.com) portion of the HTTP request and requesting the HTML document "ad1.html" from the third party server 40 at the designated URL (www.tp1.com/ad/ad1.html).

The first time the privacy server 30 requests resources from the third party server 40, the third party will assign the user (via the privacy server) a new user ID and send a cookie (e.g., TP-ID=345, Domain = tp1.com). The user ID along with other information related to the user is recorded in the third party database 42. Rather than store the cookie, the privacy server is operable to rewrite the cookie and store it on the user PC & Web Browser 10. The privacy server embeds the third party cookie information (associated with the tp1.com domain) into a in a privacy server cookie having a new "name = value" pair associated with the privacy server domain, cp.com (e.g., PP_tp1.com_TP-ID = 345, Domain = cp.com).

In subsequent requests for resources to the third party, the privacy server receives the privacy server cookie and re-formats the information (e.g., TP-ID = 345, Domain = t,p1.com). The URL of the third party resource (www.tp1.com/ad/ad1.html) is based on or derived from the content provider server resource (HTML). The privacy server strips the URL from the "Iframe Src" call and transmits a privacy server request for resources to the third party server 40 and includes the re-formatted privacy server cookie. See Figure 5, block 240. Communications between the privacy server 30 and the third party server 40 are shown generally by arrows 80.

The third party server 40 receives the privacy server request for resources and cookie and returns a third party resource (e.g., an HTML document for advertiser ad1). See Figure 5, block 250. The privacy server 30 receives the third party server resource and generates the privacy server resource based on the third party server resource. The privacy server detects whether the third party resource is an image or an HTML document. See Figure 5, block 262. If the resource is an HTML document (Rich Media) the third party resource is parsed by the privacy server for embedded calls to third party

servers (for additional HTML or images). All embedded calls are rewritten to address the privacy server 30. See Figure 5, block 264.

The privacy server returns a copy of the rewritten third party server resource to the user's Web Browser. See Figure 3, block 266. The user's Browser receives the privacy server resource (e.g., an image, pointer to an image or HTML document) and presents it to the user as part of the cp.com Web page. See Figure 3, block 270. Each additional request for resource is processed in repeated iterations as set out above until the entire Rich Media advertisement is displayed to the user.

Advantages of the Invention

Numerous advantages are provided by employing the present invention, a non-exhaustive list is disclosed below. The present invention provides a system and method for limiting the amount of information exchanged between an Internet World Wide Web user and an advertisement information provider. The invention also provides a privacy server operable to transfer advertisement information between a third party server and the user. The invention also provides a means for requesting the advertisement information from the third party server via a pre-formatted embedded request for resources to a privacy server. Pre-formatting is independent of the user and requires no user intervention. The invention also provides a system and method for limiting the amount of information exchanged between an Internet World Wide Web user and an advertisement information provider without appreciably degrading network performance. These and other advantages are readily apparent, the scope of the invention as claimed is by no means limited to or by the precise advantages recited above.

All publications and references, including but not limited to patents and patent applications, cited in this specification are herein incorporated by reference in their entirety as if each individual publication or reference were specifically and individually indicated to be incorporated by reference herein as being fully set forth. Any patent application to which this application claims priority is also incorporated by reference herein in its entirety in the manner described above for publications and references.

While this invention has been described with an emphasis upon preferred embodiments, it will be obvious to those of ordinary skill in the art that variations in the preferred devices and methods may be used and that it is intended that the invention may be practiced otherwise than as specifically described herein. Accordingly, this invention includes all modifications encompassed within the spirit and scope of the invention as defined by the claims that follow.

What is claimed:

1. A data network communication system for presenting resources to a user comprising:

a user network processing device operable to transmit at least a first and second user request for resources and present resources served in response to the first and second user requests for resources to the user;

a first server operable receive the first user request for resources and transmit at least one first server resource to the user network processing device in response to the first user request for resources;

a privacy server operable to receive the second user request for resources and transmit at least one privacy server resource to the user network processing device in response to the second user request for resources; and

a third server operable to receive a privacy server request for resources and transmit at least one third server resource to the privacy server, the privacy server being operable to receive the third server resource and generate the privacy server resource based on the third server resource.

2. The system of claim 1 wherein the user network processing device has at least one memory area operable to store at least one user tag having at least one associated data value wherein the first server is operable to read data from the user tag and write data to the user tag.

3. The system of claim 1 wherein the user network processing device has at least one memory area operable to store at least one privacy server tag having at least one associated data value and the privacy server is operable to read data from the privacy server tag and write data to the privacy server tag.

4. The system of claim 1 wherein the privacy server has a privacy server database and at least one memory area operable to store at least one privacy server tag having at least one associated data value, the privacy server being operable to store in the privacy server tag data from the third server and transmit the privacy server tag to the third server.

5. The system of claim 3 wherein the third server has a third server database wherein the third server is operable to read data from the privacy server tag, write data to the privacy server tag and store data based on at least one of the privacy server tag and the privacy server request for resources in the third server database.

6. The system of claim 1 wherein the third server resource is advertisement data and the privacy server resource is based on the advertisement data.

7. The system of claim 1 wherein the data network is the Internet and the user network processing device has a Web Browser operable to transmit at least a first and second user request for resources and present resources served in response to the first and second user request for resources to the user.

8. The system of claim 7 wherein the second user request for resources is based on the first server resource.

9. The system of claim 7 wherein the first server is operable to transmit an HTML document in response to the first user request for resources and the privacy server is operable to transmit advertisement data in response to the second user request for resources.

10. The system of claim 1 wherein the data network is the Internet and the user network processing device has a Web Browser having at least one associated memory area operable to store at least one user cookie having at least one associated data value and the first server is operable to read data from the user cookie and write data to the user cookie.

11. The system of claim 10 wherein the Web Browser has at least one memory area operable to store at least one privacy server cookie having at least one associated data value and the privacy server is operable to read data from the privacy server cookie and write data to the privacy server cookie.

12. The system of claim 10 wherein the privacy server has a privacy server database and at least one memory area operable to store at least one privacy server cookie having at least one associated data value, the third server being operable to read the data from the privacy server cookie and write data to the privacy server cookie.

13. The system of claim 10 wherein the third server has a third server database, the third server being operable to read data from the privacy server cookie, write data to the privacy server cookie and store data based on at least one of the privacy server cookie and the privacy server request for resources in the third server database.

14. The system of claim 10 wherein the third server resource is at least one of an image resource and an HTML resource having at least one embedded call addressed to the third server, the privacy server is operable to parse the HTML resource and rewrite the embedded call to address the privacy server.

15. A method for use in a computer network, having a user network processing device, first server, privacy server and a third server, a method of exchanging information between a network user and the third server, the method comprising:

transmitting a first user request for resources from the user network processing device to the first server;

transmitting at least one first server resource in response to the first user request for resources from the first server to the user network processing device;

transmitting a second user request for resources from the user network processing device to the privacy server;

transmitting a privacy server request for resources in response to the second user request for resources from the privacy server to the third server;

transmitting a third resources in response to privacy server request for resources from the third server to the privacy server;

transmitting a privacy server resource based on the third resource to the user network processing device, wherein the user network processing device is operable to present the first server resource and privacy server resource to the user.

16. The method of claim 15 further comprising storing at least one user tag in a first user network processing device memory location, the first server being operable to read data from the user tag and write data to the user tag.

17. The method of claim 15 further comprising storing at least one privacy server tag in a second user network processing device memory location, the privacy server being operable to read the data from the privacy server tag and write data to the privacy server tag.

18. The method of claim 15 further comprising storing at least one user tag in a first user network processing device memory location and storing at least one privacy server tag in a second user network processing device memory location, wherein the third server is operable to read data from the privacy server tag and write data to the privacy server tag and wherein the third server is not operable to read data from the user tag and write data to the user tag.

19. The method of claim 15 further comprising storing at least one privacy server tag in a privacy server database, the third server being operable to read data from the privacy server tag and write data to the privacy server tag.

20. The method of claim 17 wherein the third server is operable to read data from the privacy server tag, write data to the privacy server tag and store data based on at least one of the privacy server tag and the privacy server request for resources in a third server database.

21. The method of claim 15 wherein the second user request for resources is based on the first server resource.

22. The method of claim 15 wherein the privacy server is operable to transmit advertisement data in response to the second user request for resources.

23. The method of claim 15 further comprising rewriting at least one embedded request for resources addressed to the third server contained within the first server resource to an embedded request for resources addressed to the privacy server.

24. The method of claim 15, further comprising measuring a time interval between the transmission of the privacy server request for resources and receipt of the third server resource.

25. The method of claim 24, further comprising transmitting a second privacy server request for resources to a fourth server if the time interval is greater that a performance criterion, the fourth server being operable to transmit a fourth server resource to the privacy server, wherein the privacy server resource is based on the fourth server resource.

26. The method of claim 24, further comprising transmitting a second privacy server request for resources to the first server if the time interval is greater than a performance criterion, the first server being operable to transmit a substitute resource to the privacy server, wherein the privacy server resource is based on the substitute resource.

27. The method of claim 24, wherein the privacy server is operable to initiate a corrective action if the time interval is greater that a performance criterion.

28. The method of claim 24, wherein the privacy server is operable to store the time interval in a privacy server database.

29. The method of claim 24, wherein the privacy server is operable to transmit the time interval to another server.

30. The method of claim 15, wherein the third server resource is at least one of an image resource and an HTML resource having at least one embedded HTML call addressed to the third server, the privacy server being operable to parse the HTML resource and rewrite the embedded HTML call to address the privacy server.

31. A privacy server in data communication with an Internet user, the privacy server being operable to:

(1) receive and identify a user request for resources directed to the privacy server as intended for forwarding to a third server;

(2) format a privacy server request for resources based on the user request for resources to the third server;

(3) transmit the privacy server request for resources to the third server;

(4) receive a third resource from the third server in response to the privacy server request for resources; and

(5) transmit a privacy server resource based on the third resource.

32. The privacy server of claim 31, wherein the privacy server is operable to store a privacy server cookie transmitted by the third server.

33. The privacy server of claim 32, wherein the third server resource is at least one of an image resource and an HTML resource having at least one embedded call addressed to the third server, the privacy server being operable to parse the HTML resource and rewrite the embedded call to address the privacy server.

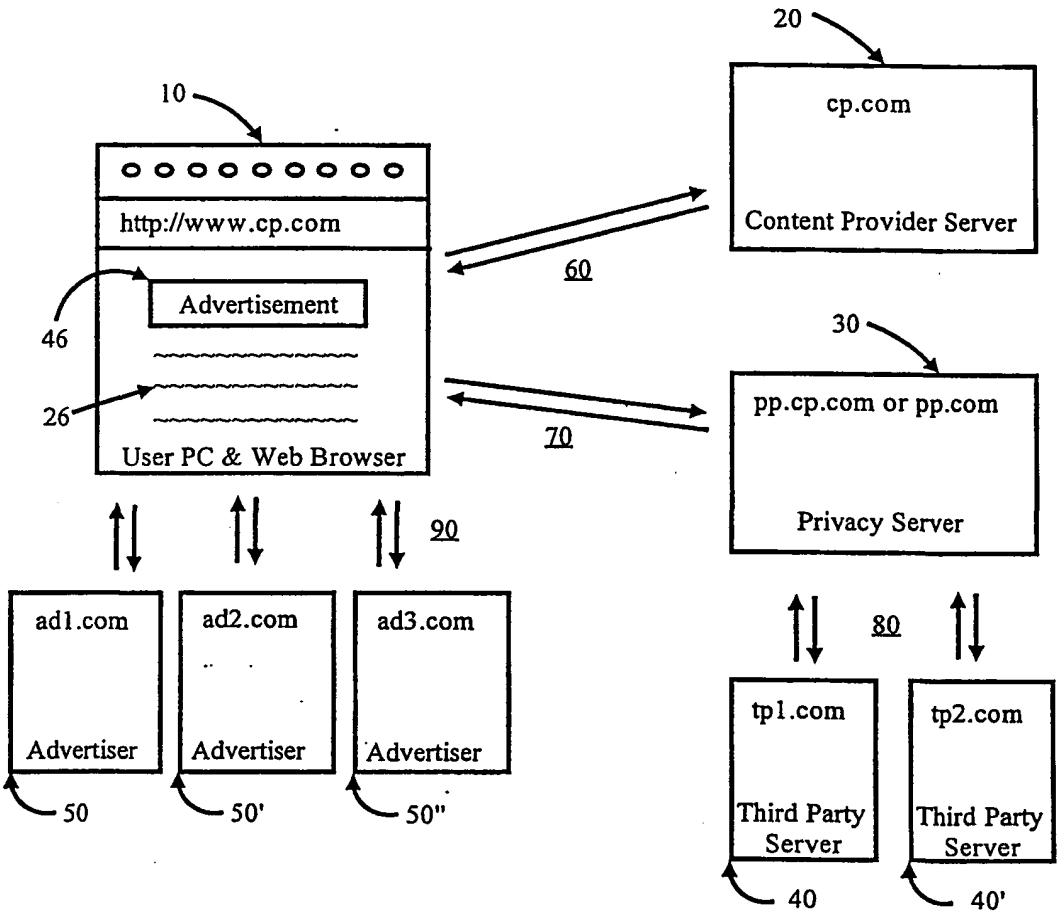

20
cp.com
Content Provider Server
10
http://www.cp.com
Advertisement
46
26
User PC & Web Browser
60
30
pp.cp.com or pp.com
Privacy Server
70
90
80
ad1.com
Advertiser
ad2.com
Advertiser
ad3.com
Advertiser
50
50'
50"
tp1.com
Third Party Server
tp2.com
Third Party Server
40
40'

FIGURE 1

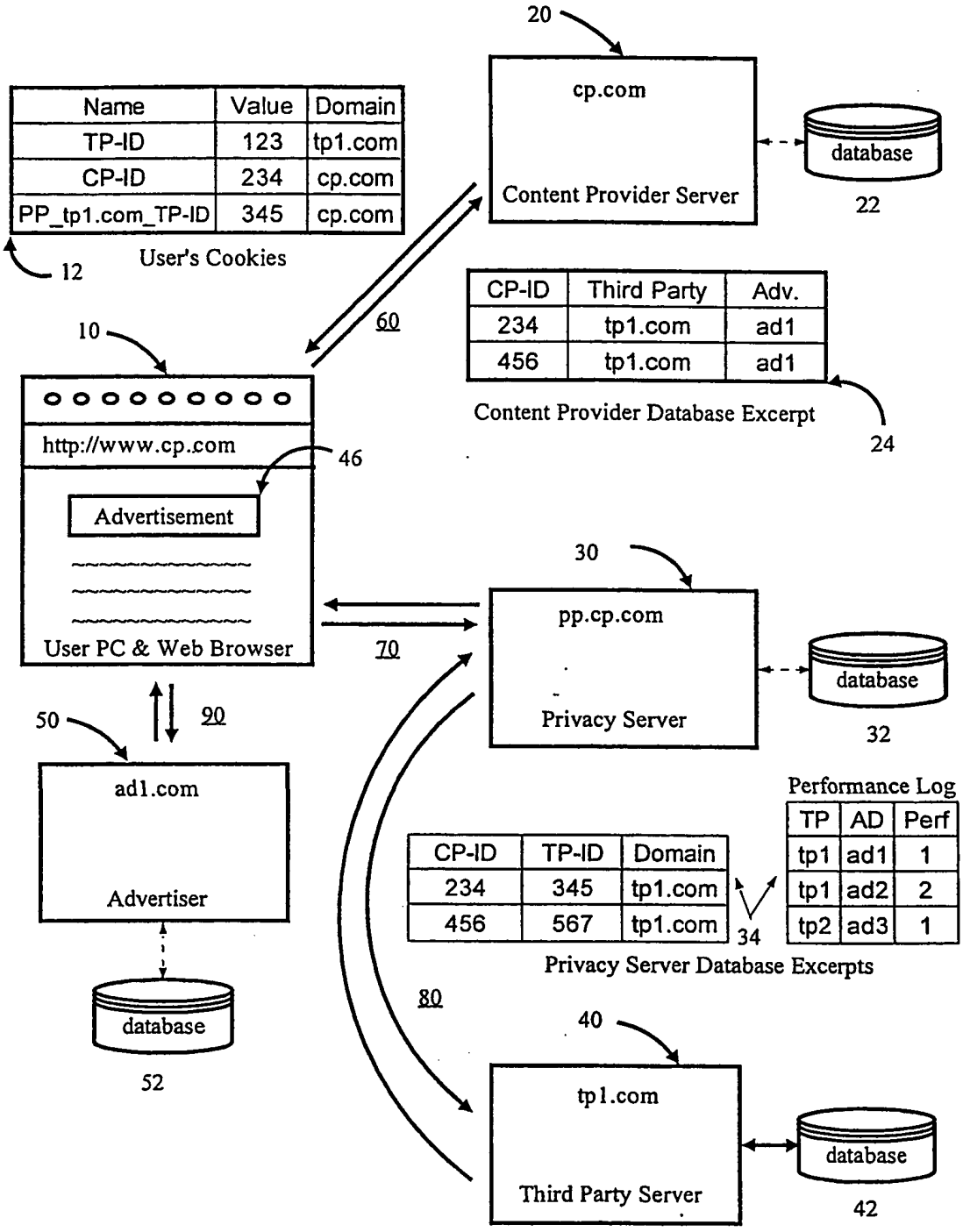

20
cp.com
Content Provider Server
database
22
Name | Value | Domain
TP-ID | 123 | tp1.com
CP-ID | 234 | cp.com
PP_tp1.com_TP-ID | 345 | cp.com
User's Cookies
12
60
CP-ID | Third Party | Adv.
234 | tp1.com | ad1
456 | tp1.com | ad1
Content Provider Database Excerpt
24
10
http://www.cp.com
46
Advertisement
User PC & Web Browser
30
pp.cp.com
Privacy Server
database
32
70
90
50
ad1.com
Advertiser
database
52
Performance Log
TP | AD | Perf
tp1 | ad1 | 1
tp1 | ad2 | 2
tp2 | ad3 | 1
CP-ID | TP-ID | Domain
234 | 345 | tp1.com
456 | 567 | tp1.com
34
Privacy Server Database Excerpts
80
40
tp1.com
Third Party Server
database
42
TP-ID | Referring Site | Adv. | CT
123 | cp.com | ad1 | N
345 | cp.com | ad1 | Y
345 | cp.com | ad2 | N
567 | cp.com | ad1 | N
Third Party Database Excerpt
44

FIGURE 2

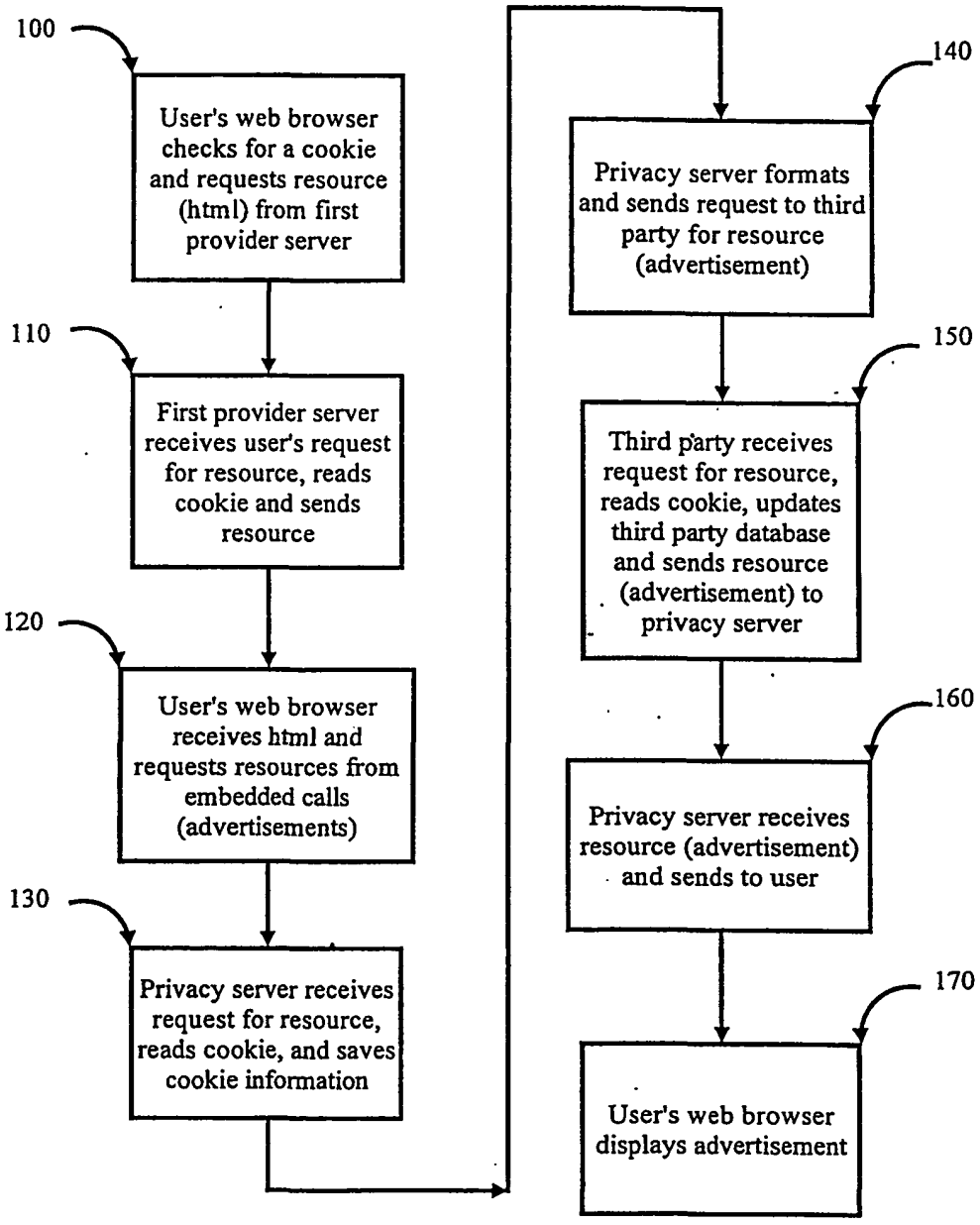

100
User's web browser checks for a cookie and requests resource (html) from first provider server
110
First provider server receives user's request for resource, reads cookie and sends resource
120
User's web browser receives html and requests resources from embedded calls (advertisements)
130
Privacy server receives request for resource, reads cookie, and saves cookie information
140
Privacy server formats and sends request to third party for resource (advertisement)
150
Third party receives request for resource, reads cookie, updates third party database and sends resource (advertisement) to privacy server
160
Privacy server receives resource (advertisement) and sends to user
170
User's web browser displays advertisement

FIGURE 3

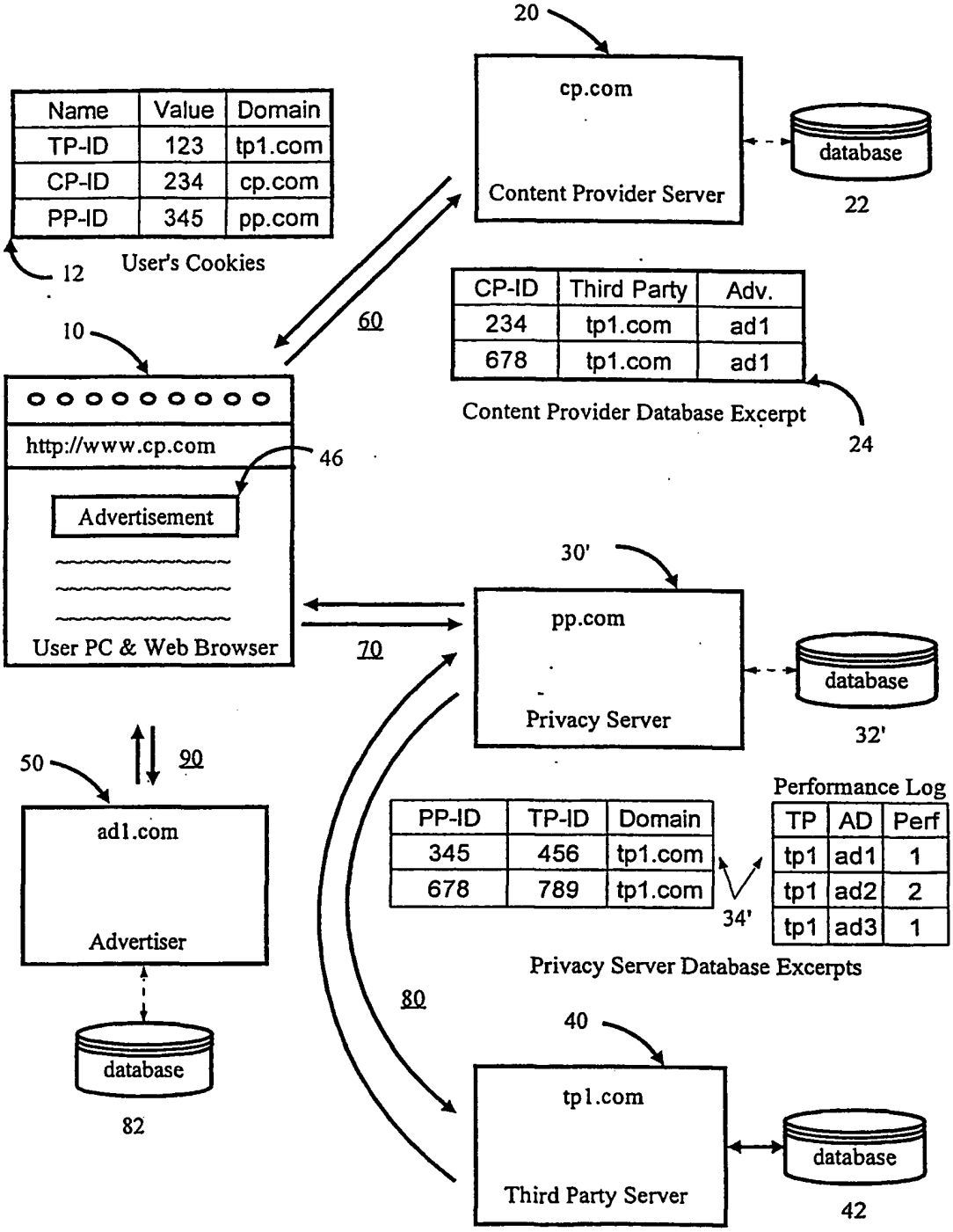

20
cp.com
Content Provider Server
database
22
Name | Value | Domain
TP-ID | 123 | tp1.com
CP-ID | 234 | cp.com
PP-ID | 345 | pp.com
12
User's Cookies
60
CP-ID | Third Party | Adv.
234 | tp1.com | ad1
678 | tp1.com | ad1
Content Provider Database Excerpt
24
10
http://www.cp.com
46
Advertisement
User PC & Web Browser
30'
pp.com
Privacy Server
database
32'
70
50
90
ad1.com
Advertiser
database
82
PP-ID | TP-ID | Domain
345 | 456 | tp1.com
678 | 789 | tp1.com
34'
Performance Log
TP | AD | Perf
tp1 | ad1 | 1
tp1 | ad2 | 2
tp1 | ad3 | 1
Privacy Server Database Excerpts
80
40
tp1.com
Third Party Server
database
42
TP-ID | Referring Site | Adv. | CT
123 | cp.com | ad1 | N
456 | cp.com | ad1 | Y
456 | cp.com | ad2 | N
789 | cp.com | ad1 | N
Third Party Database Excerpt
44

FIGURE 4

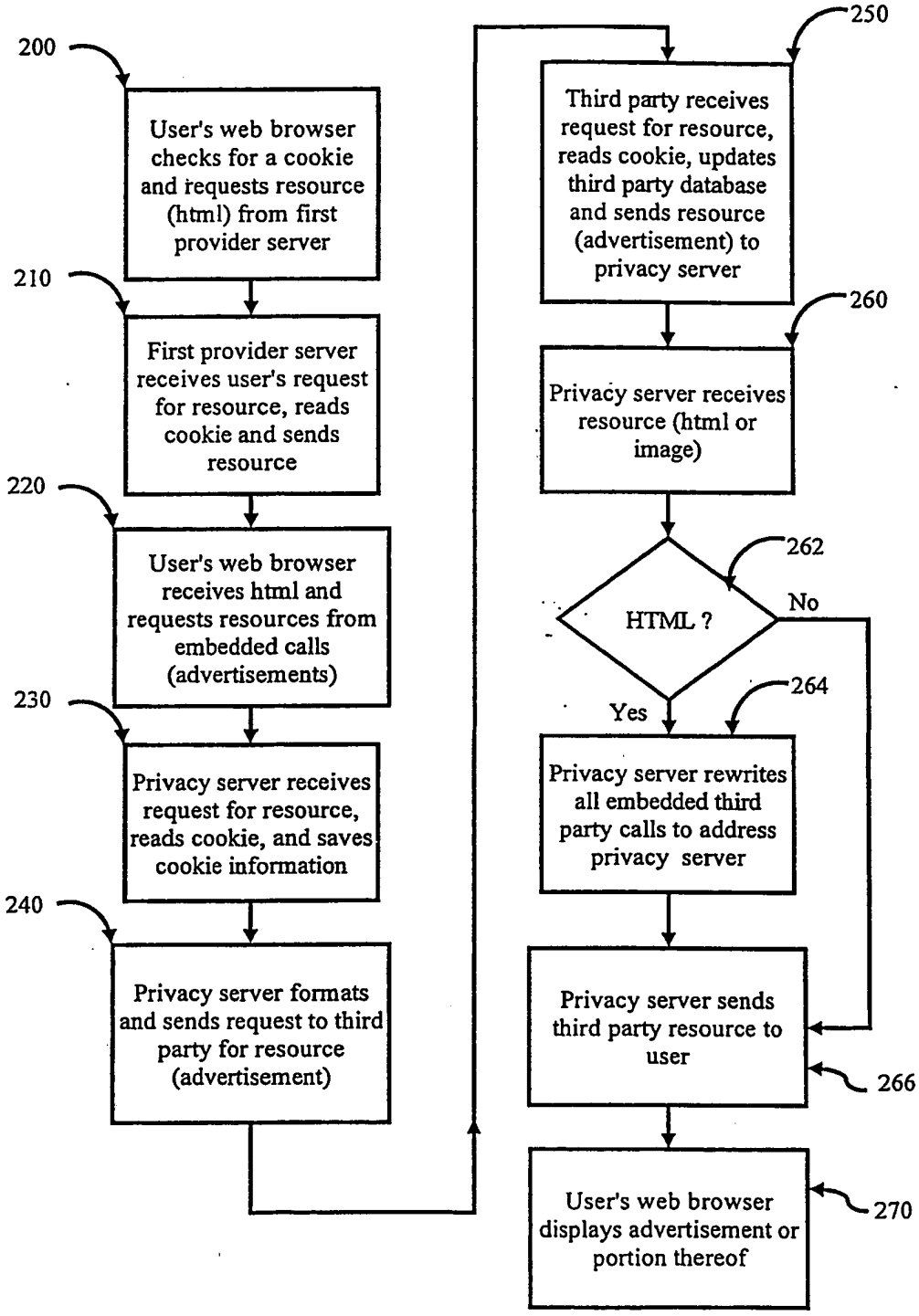

200
User's web browser checks for a cookie and requests resource (html) from first provider server
210
First provider server receives user's request for resource, reads cookie and sends resource
220
User's web browser receives html and requests resources from embedded calls (advertisements)
230
Privacy server receives request for resource, reads cookie, and saves cookie information
240
Privacy server formats and sends request to third party for resource (advertisement)
250
Third party receives request for resource, reads cookie, updates third party database and sends resource (advertisement) to privacy server
260
Privacy server receives resource (html or image)
262
HTML ?
No
Yes
264
Privacy server rewrites all embedded third party calls to address privacy server
Privacy server sends third party resource to user
266
User's web browser displays advertisement or portion thereof
270

FIGURE 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/20340

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 17/60
US CL :705/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searchec

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Dialog: cookies, proxy, privacy, advert?

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim
Y	US 5,961,593 A (GABBER et al) 05 October 1999, entire document.	1-33
Y	US 5,948,061 A (MERRIMAN et al) 07 September 1999, entire document.	1-33

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priorit date and not in conflict with the application but cited to understand th principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot b considered novel or cannot be considered to involve an inventive ste when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)		
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 SEPTEMBER 2001	18 OCT 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JEFFREY D. CARLSON R. Matthews Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (July 1998)★